



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/787,262

02/27/2004

Kunihiko Miyazaki

64235-016

1288

20277 7590 12/28/2007
MCDERMOTT WILL & EMERY LLP
600 13TH STREET, N.W.
WASHINGTON, DC 20005-3096

EXAMINER

WYSZYNSKI, AUBREY H

ART UNIT

PAPER NUMBER

2134

MAIL DATE

DELIVERY MODE

12/28/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/787,262

Applicant(s)

MIYAZAKI ET AL.

Examiner

Aubrey H. Wyszynski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-15 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 2/27/04 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- 1) ☒ Certified copies of the priority documents have been received.
 - 2) ☐ Certified copies of the priority documents have been received in Application No. _____.
 - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 8/1/07, 7/26/06, 7/15/04.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-15 are pending.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 7/15/04, 7/26/06 and 8/1/07 are being considered by the examiner.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-5 and 11-14 are rejected under 35 U.S.C. 102(b) as being anticipated by Ron Steinfeld, Laurence Bull, and Yuliang Zheng, "Content Extraction Signatures", (hereinafter Steinfeld).

Regarding claims 1, Steinfeld discloses an electronic document authenticity assurance method comprising the steps of: dividing an electronic document into a plurality of

constituent elements; and affixing electronic signatures to all subsets of a set including the plurality of constituent elements (page 287, 2.1 describes Content Extraction Signature (CES), dividing a document into portions or sub messages and runs an extract algorithm to produce an extracted signature, also page 286 describes signing portions of a document).

Regarding claim 2, Steinfeld discloses an electronic document authenticity assurance method comprising the steps of:

dividing an electronic document into a plurality of constituent elements;
creating data in which information specifying a relationship between each of the plurality of constituent elements and a structure of the electronic document is bound to a respective one of the plurality of constituent elements; and
affixing an electronic signature to the bound data (Steinfeld discloses all the elements described above in claim 1 and further discloses a "Content Extraction Access Structure (CEAS), the encoding of the subsets of sub messages indexes in the original document which the signer can use to specify w which extracted subdocuments the user is allowed to extract valid signatures for, page 293, first ¶ and page 291 second ¶).

Regarding claim 3, Steinfeld discloses electronic document authenticity assurance method comprising the steps of:

dividing an electronic document into a plurality of constituent elements;

creating data in which hash values respectively calculated on the plurality of constituent elements by means of a cryptographic hash function are bound to the respective plurality of constituent elements; and affixing an electronic signature to the bound data (Steinfeld further discloses hash values on page 294, first ¶ and pages 295-296, A Variant: Scheme HashTree; Extraction consists of appending to the signature the hash values associated with intermediate tree nodes which are required in order to compute the root has value from the commitments of the extracted submessages in the subdocument).

Regarding claim 4, Steinfeld discloses an electronic document authenticity assurance method comprising the steps of:

dividing an electronic document into a plurality of constituent elements;
generates and binds random-numbers to the respective constituent elements;
creating data in which hash values respectively calculated on the plurality of random-numbered constituent elements by means of a cryptographic hash function are bound to the respective plurality of random-numbered constituent elements; and
affixing an electronic signature to the bound data (page 296, first ¶, the randomness values for the extracted submessage are also appended).

Regarding claim 5, Steinfeld discloses an electronic document disclosure system comprising:

an original document creator unit which divides an electronic document into a plurality of constituent elements, affixes electronic signatures to all subsets of a set including the plurality of constituent elements,

and stores the resultant electronic document into a document management unit (page 288, fig. 1, university A creates original document and page 287, second ¶, The university uses the Sign algorithm of a CES scheme to sign the original document, divided into portions (submessages) and produce a content extraction signature, given to student B along with the full document);

a disclosure document creator unit which takes out a disclosure object document from among electronic documents stored in the document management unit, at the time of acceptance of an information disclosure request, creates a disclosure document in which information not to be disclosed is omitted from the disclosure object document, and sends the disclosure document to a recipient unit; and

the recipient unit which verifies a signature of an original document creator at the time of acceptance of the disclosure document which is made published (fig. 1, Student B and Prospective Employers C and D; and page 287, second ¶, The student then extracts a *subdocument A'* of the original document consisting of a selected subset of the document submessages (e.g. not including *m1*, the DOB of B, but including all other submessages) He then runs an Extract algorithm of the CES scheme to produce an *extracted signature* by the university A for the extracted subdocument A'. Student B then forwards the subdocument A' and the extracted signature for A'. The employer uses the Verify algorithm of the CES to verify the extracted signature on A').

Regarding claims 11, Steinfeld discloses a method which discloses an electronic document to which an electronic signature is affixed in accordance with an electronic document authenticity assurance method according to any one of claims 1 to 4, comprising the steps of:

designating as a disclosure object document the electronic document to which the electronic signature is affixed (fig. 1, page 288, Original document);
creating a disclosure document in which information not to be disclosed is omitted from the disclosure object document (fig. 1, subdocument A and subdocument B); and
further affixing a signature to the disclosure document (page 287, 2.1).

Regarding claim 12, Steinfeld discloses an electronic document disclosure system according to claim 5, wherein, the disclosure document creator unit affixes another signature of the disclosure document creator unit to the disclosure document in which the information not to be disclosed is omitted (page 287, 2.1).

Regarding claim 13, Steinfeld discloses an electronic document authenticity assurance method comprising the steps of: dividing an electronic document into a plurality of constituent elements;
creating data indicative of undisclosure and respectively corresponding to the plurality of constituent elements;

calculating signature object data related to the plurality of constituent elements, from the plurality of constituent elements and the data indicative of undisclosure and respectively corresponding to the plurality of constituent elements;

binding together the calculated signature object data; and

affixing an electronic signature to the bound data (page 287, 2.1 and page 288, fig. 1).

Regarding claim 14, Steinfeld discloses an electronic document disclosure method comprising the steps of:

if first information not to be disclosed is included in constituent elements which constitute a signed electronic document created in accordance with

an electronic document authenticity assurance method according to claim 13, omitting constituent elements corresponding to the first information and leaving data indicative of undisclosure corresponding to the first information;

if second information to be disclosed and not to be made undisclosed in future is included in the constituent elements, leaving constituent elements corresponding to the second information and omitting data indicative of undisclosure corresponding to the second information; and

if third information to be disclosed and to be made undisclosed in future is included in the constituent elements, leaving both constituent elements and data indicative of undisclosure corresponding to the third information (page 287, 2.1 and page 288, fig. 1, demonstrates original document containing components m_1 through m_n , and

subdocuments A and B which contain only a few components so that sever of the components are not discloses to the prospective employers).

5. Claims 6-8 are rejected under 35 U.S.C. 102(e) as being anticipated by Brown et al, US 6,671,805.

Regarding claim 6, Brown discloses an electronic document authenticity assurance method using a unit of a third-party organ, comprising the steps of:
dividing an electronic document into a plurality of constituent elements (col. 5, lines 13-29); and depositing all subsets of a set including the plurality of constituent elements into the unit of the third-party organ as assurance object information (fig. 2, #204 storage device and col. 9, lines 55-60 and col. 14, lines 5-36).

Regarding claim 7, Brown discloses an electronic document authenticity assurance method using a unit of a third-party organ, comprising the steps of:
dividing an electronic document into a plurality of constituent elements (fig. 1, #106, parser);
creating data in which information specifying a relationship between each of the plurality of constituent elements and a structure of the electronic document is bound to a respective one of the plurality of constituent elements (col. 8, lines 35-47, tags); and
depositing the created data into the unit of the third-party organ as assurance object information (fig. 2, #204 and col. 9, lines 52-60).

Regarding claim 8, Brown discloses an electronic document authenticity assurance method using a unit of a third party organ, comprising the steps of:
dividing an electronic document into a plurality of constituent elements;
calculating hash values on the plurality of constituent elements respectively by means of a cryptographic hash function and depositing data in which the calculated hash values are bound together into the unit of the third-party organ as assurance object information (col. 9, lines 3-20 and col. 13, lines 52-60).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Steinfeld in view of Brown and further in view of Bush et al, US 6,936,971.

Regarding claim 9, Steinfeld discloses an electronic document authenticity assurance method comprising the steps of:
dividing an electronic document into a plurality of constituent elements (page 287, 2.1 describes Content Extraction Signature (CES), dividing a document into portions or sub

messages and runs an extract algorithm to produce an extracted signature, also page 286 describes signing portions of a document);

generating random numbers for the respective plurality of constituent elements and binding the random numbers to the respective plurality of constituent elements (page 296, first ¶, the randomness values for the extracted submessage are also appended); and calculating hash values on the respective plurality of constituent elements to which the respective random numbers are bound, by means of a cryptographic hash function (Steinfeld further discloses hash values on page 294, first ¶ and pages 295-296, A

Variant: Scheme HashTree; Extraction consists of appending to the signature the hash values associated with intermediate tree nodes which are required in order to compute the root has value from the commitments of the extracted submessages in the subdocument). Steinfeld lacks or does not expressly disclose depositing data in which the calculated hash values are bound together into a unit of a third-party organ as assurance object information. However, Brown discloses depositing data in which the calculated hash values are bound together into a unit of a third-party organ as assurance object information (fig. 2, #204 storage device and col. 9, lines 55-60 and col. 14, lines 5-36). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Steinfeld with the method of Brown to deposit the data as assurance object information in order to compare future documents to the original document, as taught by Brown, (fig. 8C, document template stored in storage device 204).

Regarding claim 10 Steinfeld in view of Brown disclose an electronic document disclosure system. Steinfeld in view of Brown lacks or does not expressly disclose a document management unit.

However, Bush discloses an original document creator unit (sender, fig. 1, #100, fig. 2, #196 and fig. 9) which deposits assurance object information into a unit of a third-party organ with regard to a created electronic document in accordance with an electronic document authenticity assurance method using the third-party organ, according to any one of claims 6 to 9, and stores the assurance object information into a document management unit (distribution agent, fig. 1, #140-150 and fig. 2, #233);

a disclosure document creator unit (authentication agent, fig. 1, #105-155 and fig. 2, #215) which takes out a disclosure object document (abstract) from among electronic documents stored in the document management unit, at the time of acceptance of an information disclosure request (fig. 5, #505, recipient requests authenticated document from distribution agent),

creates a disclosure document (authenticated document) in which information not to be disclosed is omitted from the disclosure object document, and sends the disclosure document to a recipient unit (fig. 9, #512); and the recipient unit which requests the unit of the third-party organ to verify the authenticity of the disclosure document, at the time of acceptance of the disclosure document which is published (fig. 5, demonstrates the interaction between the recipient, sender, authentication agent and the distribution agent). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Steinfeld in view of Brown with the system

of Bush to include a document management unit in order to have a system that registers electronic documents and validates sender and recipient identities, as taught by Bush (abstract).

8. Claim 15 rejected under 35 U.S.C. 103(a) as being unpatentable over Steinfeld as applied to claim 13 above, and further in view of Bush.

Regarding claim 15, Steinfeld discloses an electronic document disclosure system comprising:

an original document creator unit which affixes an electronic signature to a created electronic document in accordance with an electronic document authenticity assurance method according to claim 13, and stores the obtained original document into a document management unit;

a disclosure document creator unit (fig. 1, original document, University A) which takes out

a disclosure object document from among electronic documents stored in the document management unit, at the time of acceptance of an information disclosure request, and creates a disclosure document in which:

if first information not to be disclosed is included in constituent elements included in the disclosure object document, constituent elements corresponding to the first information are omitted and data indicative of undisclosure corresponding to the first information are left;

if second information to be disclosed and not to be made undisclosed in future is included in the disclosure object document, constituent elements corresponding to the second information are left and data indicative of undisclosed corresponding to the second information are omitted; and

if third information to be disclosed and to be made undisclosed in future is included in the disclosure object document, both constituent elements and data indicative of undisclosed corresponding to the third information are left (Steinfeld further discloses hash values on page 294, first ¶ and pages 295-296, A Variant: Scheme HashTree; Extraction consists of appending to the signature the hash values associated with intermediate tree nodes which are required in order to compute the root has value from the commitments of the extracted submessages in the subdocument.), and the disclosure document is created and is sent to a recipient unit (potential employer).

Steinfeld lacks or does not expressly disclose a document management unit and a recipient unit which verified the authenticity of the original document. However, Bush discloses a document management unit (distribution agent, fig. 1, #140-150 and fig. 2, #233) and the recipient unit (fig. 9, #512) which verifies the authenticity of an original document creator, at the time of acceptance of the disclosure document which is published (fig. 5, demonstrates the interaction between the recipient, sender, authentication agent and the distribution agent to verify the authenticity of the document). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Steinfeld in view of Brown with the system

of Bush to include a document management unit and recipient to verify the authenticity of the original document in order to have a system that registers electronic documents and validates sender and recipient identities, as taught by Bush (abstract).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Wyszynski whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 5712723811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number:
10/787,262
Art Unit: 2134

Page 15

AHW

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


12,24,07